ISSN: 2277-9655
Impact Factor: 4.116

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

POWER THEFT PREVENTION SYSTEM VIA REMOTE MONITORING

Bigyan Basnet, Dileep Kumar Appana*, Arjun Prasad Kandel, Narayan Poudel
Department of Electrical Engineering, Advanced College of Engineering, Nepal.
* Lead Project Engineer, Enersys Energy Solutions Hyderabad, India.
Department of Electrical Engineering, Advanced College of Engineering, Nepal.
Department of Electrical Engineering, Advanced College of Engineering, Nepal.

DOI: 10.5281/zenodo.60101

ABSTRACT

Energy is indispensable in our daily routines, which lead to monitoring of illegal usage of electrical power. Here we deployed radio communication and microcontroller system technologies together for detecting pilferage of power consumption, its control and signaling alerts to local substation to make an efficient real time power monitoring system. The complete operation, detecting and controlling is divided in to transmitting and receving sections, where the former is deployed at the consumer end and the later at electrical substation. The implementation of the automotive system includes an ATMEGA644P microcontroller, GSM to transmit the collected parameters from sensors (current, voltage, frequency) in the transmitting end. The monitored output will be displayed on a PC at the local substation which is at a remote place. Based on the received information, controlling operation is performed.

KEYWORDS: Electrical Power Theft, GSM, Remote Monitoring, Current Sensors, ATMEGA644P.

INTRODUCTION

Control on Electricity theft is inevitable because of its impact on the cost of electricity to consumers and stability of utility companies. The common Electricity theft can be in the form of meter tampering, stealing, illegal connections like hookups, bypass, billing irregularities, and unpaid bills.

Electrical power theft is the main cause of Non- Technical Losses (NTL) in the electrical power system. The NTL comprises of illegal connections, meter tampering, billing errors etc. out of which electricity theft through meter tampering and direct rigging from the transmission or the distribution line contributes higher percentage of loss of electricity [1] [2]. In United States of America, the NTL are estimated to about 0.5% to 3.5% of the gross annual revenue [3]. In developing countries like India, the loss of electricity due to theft is projected to about 20% to 30% of the overall loss in Power utility [3]. Particularly taking about Nepal, 6.2 billions of rupees was net lost in 2014/2015 fiscal year due to technical and non-technical losses. While at the same time period there was 24.4% loss against the total available electricity. Interestingly, only 15% attributed to technical loss and rest to theft. More details about the previous finiancial years are shown in Figure 1. In Figure 2, NEA report of 2011 says the loss in rupees.

Various researches have been done. Some of them are (1) Preventive measures like injection of a narrow band power line carrier signal into the distribution power line along the power frequency signal (230V, 50Hz) can be applied. (2) Detection of power theft can also be done using power line communication[3]. (3) Comparison between the total load supplied by the distribution transformer and the total load used by the consumer and the error signal is

used to identify the power theft using fuzzy logic [4]. Above all this paper presents with the inclusion of embedded based AMR and GSM technology and to indicate any type of theft at local substation. The project is technically, economically and operationally feasible.

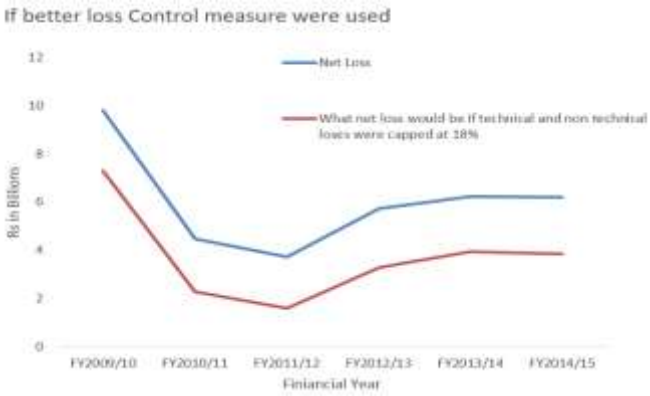

Figure 1 : Failure to plug System loss causes NEA huge loss

In general practice, measures like increasing load-shedding hours in those feeders having higher leakage, not put them in the priority list for maintenance like changing transformers, and may eventually cut off power if leakage is not controlled. But this method is not reliable since all users are treated belonging to the same feeder.

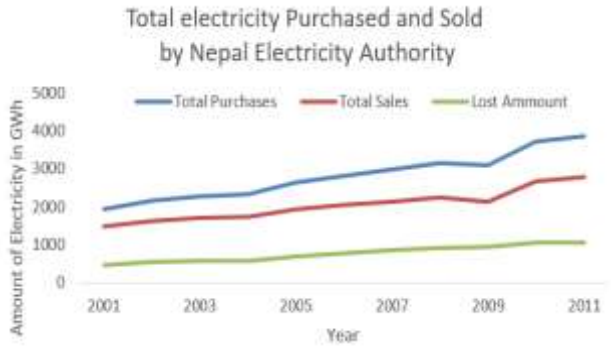

Figure 2 : NEA Annaul Report 2011

To overcome the above problem we proposes not only the effective way to detect power theft at the exact location in an accurate and cost effective way but also the real time power monitoring and transmitting the system information over wireless to local substation which minimize the cost of hiring power taskforce to monitor the activities.

METHODOLOGY FOR TAMPER DETECTION

A system for detection of tampering with a utility meter provides not only an indication that tampering has occurred but also sufficient information to enable an estimation of actual consumption to be made as opposed to the tampered meter consumption.

- **Neutral Tampering**

This tampering is done by disconnecting the neutral wire in the domestic electricity meter. With the Neutral disconnected, there is no voltage input and thus no output would be generated by the power supply. The component used for the neutral tampering detection circuit is an Optocoupler connected in parallel to the Voltage coil. When the neutral wire from the electricity meter is disconnected, the power supply to the LED is also disconnected and hence it does not glow. As long as the neutral and the phase are connected to the voltage coil, the parallely connected

Optocoupler LED produces a high output thereby biasing the base of the photo transistor which produces an output at the emitter. As soon as the LED fails to glow, the photodiode is unbiased and its output drops to low level or logic "0" signal and it sent to the micro controller.

- **Magnetic Tampering**

Magnetic tampering technique is done by bringing a high powered magnet in close proximity of the domestic electricity meter. When this happens, the rotor disc is exposed to a high magnetic field. Then the resultant opposing magnetic field to the rotor is highly increased leading to slowing down of rotor or perfect stopping of the disc rotation. The idea is to saturate the core of the sensors or distort the flux in the core so that output is erroneous. This effectively results in less billing. When a high power magnet is bought in proximity of the electricity meter in the presence of the Reed switch two leads come in contact with each other and result in the closed circuit thereby helping in detection of the signal by the micro controller. Thus the tampering is detected effectively and the micro controller receives the information, which it passes on to the LCD unit and the GSM modem.

- **Reverse Current**

Reverse Current occurs when the phase and neutral are wired to the wrong inputs, causing current to flow in the direction opposite to normal. Figure shows the Neutral Wire connection is swapped thus causing current IN to flow in the reverse direction. Due to the reverse current flow through Neutral, metering firmware will show wrong signs in active power readings. The polarity of current transformer (CT) changes when any of the two currents has a sign opposite the one expected. To overcome this, metering firmware always uses the absolute value of active power for driving the energy pulse, thus reverse current has no effect on energy calculation or accurate billing.

- **Partial Earth Fault Condition**

Partial earth fault means some of the load has been connected to another ground potential and not the neutral wire. In normal condition current going through the Phase wire is the same as coming out of the neutral wire (IP = IN). In case of partial Earth Fault Condition, the current in the neutral wire IN is less than that in the Phase or live wire IP. To detect this condition, firmware monitors the currents on both energy wires - Phase and Neutral, and compares them. If they differ significantly, the firmware uses the larger of the two currents to determine the amount of energy to be billed and signals a "fault" condition.

Our proposed system is shown in figure 3.

SYSTEM HARDWARE

- **ATMEGA644P Microcontroller**

The ATmega644p is a low-power CMOS 8-bit microcontroller based on the AVR enhanced RISC architecture. By executing powerful instructions in a single clock cycle, the ATmega644m achieves throughputs approaching 1 MIPS per MHz allowing the system design to optimize power consumption versus processing speed.

- **ADC**

It is a device that converts a continuous physical quantity (usually voltage) to a digital number that represents the quantity's amplitude. In ATmega 644p the inbuilt ADC is provided which automatically reads the signal (full wave rectified) and converts to its digital equivalent value.

ISSN: 2277-9655
Impact Factor: 4.116

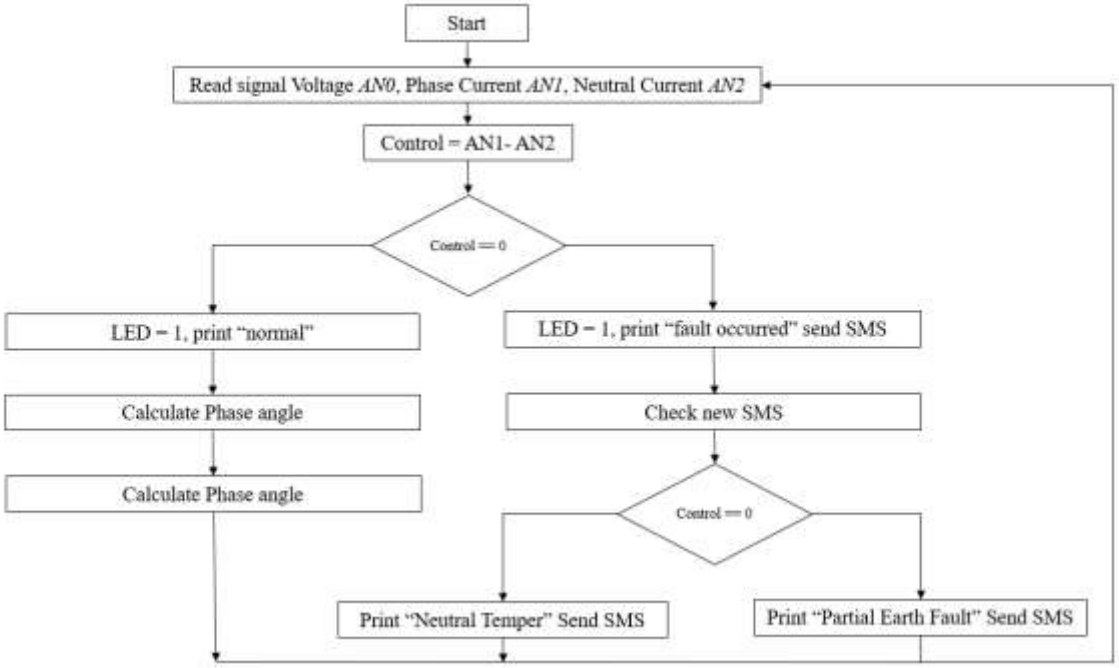

Figure 3: Flow diagram of our proposed system.

- **Current Transformer(CT)**

The Current Transformers (CT's) are instrument transformers that are utilized to supply a reduced value of current to meters, protective relays, and other instruments. A current transformer is an instrument transformer used to step down large values of currents associated with big loads, such that smaller size meters can measure the actual current of the feeder.

- **Voltage Transformer and Voltage Division**

Voltage transformer is an electromagnetic device which consists of two or more coils wound on a magnetic core and changes the voltage level in a circuit, under fixed frequency. As it is mentioned, ATmega644P microcontroller is the component, used in this project and the maximum voltage can be sensed is 5.0 V DC. The resistor values *R1, R2* in Figure above are chosen in a manner to give us a required voltage that is suitable to be fed in the MCU. These values are chosen specifically to satisfy the circuit design requirements.

$$V_{out} = V_{in} * \frac{R_1}{R_1 + R_2}$$

- **Zero Crossing Detector**

A transistor and bridge rectifier can be used as a zero cross detector. The bridge rectifier rectifies the ac input signal and this signal is fed to the base of transistor and the transistor conducts in all cases except zero signals. When the base of transistor get zero signal then transistor does not conduct and the 5V pulse is appear. According to the general theory and principles of the Power theft calculation; Power factor is the major part for the calculation of active and reactive power therefore calculation of the phase difference between current and voltage is the prime requirement. To solve this problem Zero Cross Detection method is used and after Detecting the Zero Crossed points; pulse at zero cross signals are obtained and applied to the microcontroller which can follow these rising and falling edges (it depends on the written program for microcontroller operation which in this case falling is selected) and with its ability to set or reset the related counter/timers which calculates the time difference between these two

ISSN: 2277-9655
Impact Factor: 4.116

signals. Considering the selected oscillator, prescale and frequency values; it is possible to calculate the phase difference in terms of degrees.

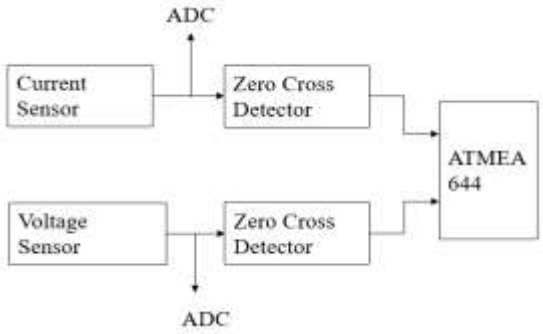

Figure 4 : Block diagram of signal input to microcontroller

- **Optocoupler**

A solid state component that uses a light-emitting diode to transmit light through an optically transparent barrier between two isolated circuits. This barrier insulates circuits by allowing light to pass through, but not current. A Liquid crystal display are interfaced to micro-controller unit that are used to display the meter reading,date time, power factor, power status, total load used etc.

- **Global System for Mobile Telecommunication(GSM)**

GSM modem is a device, which has all the protocol of GSM standards embedded into a micro controller and this function are controlled by standard AT commands of GSM technology. A unique features of Gsm is the Short Message Service (SMS) - a bidirectional service for short alphanumeric (up to 160 bytes) messages & are transported in a store-and-forward fashion.

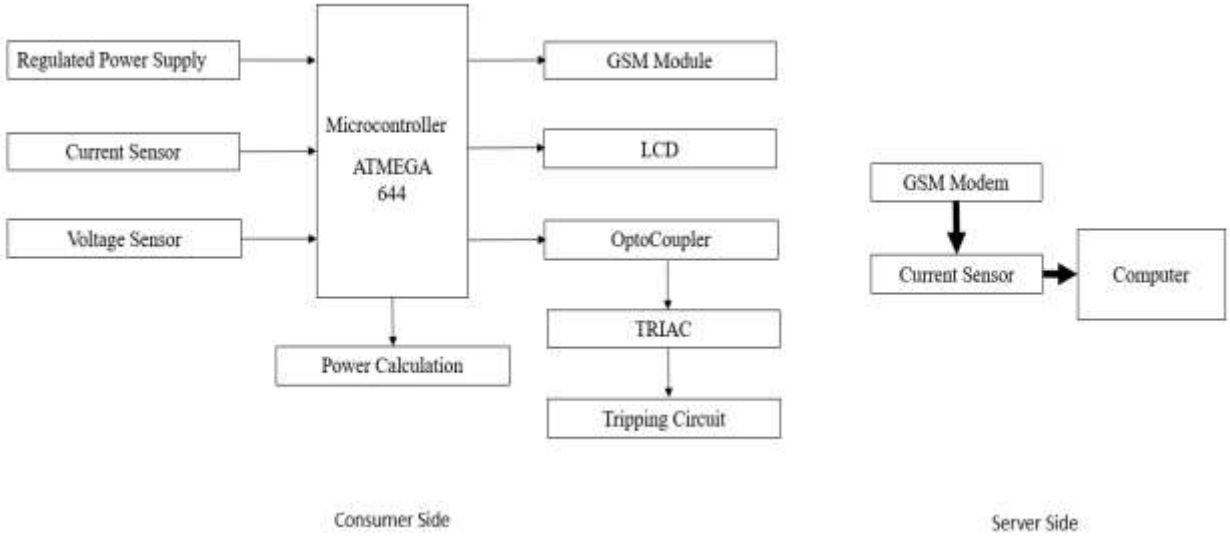

Figure 5: System architecture on Consumer and Server side

ISSN: 2277-9655
Impact Factor: 4.116

SIMULATION RESULTS AND DISCUSSION

The main task of our project is to detect, control and indicate the power fraud at exact location and transmit the information (fault and real time power) over wireless via GSM. We have completed the embedded system which provides real time data such as KW, KVA, KVAR etc. instantly when supply authority requires and automatically cut off the main circuit during theft.

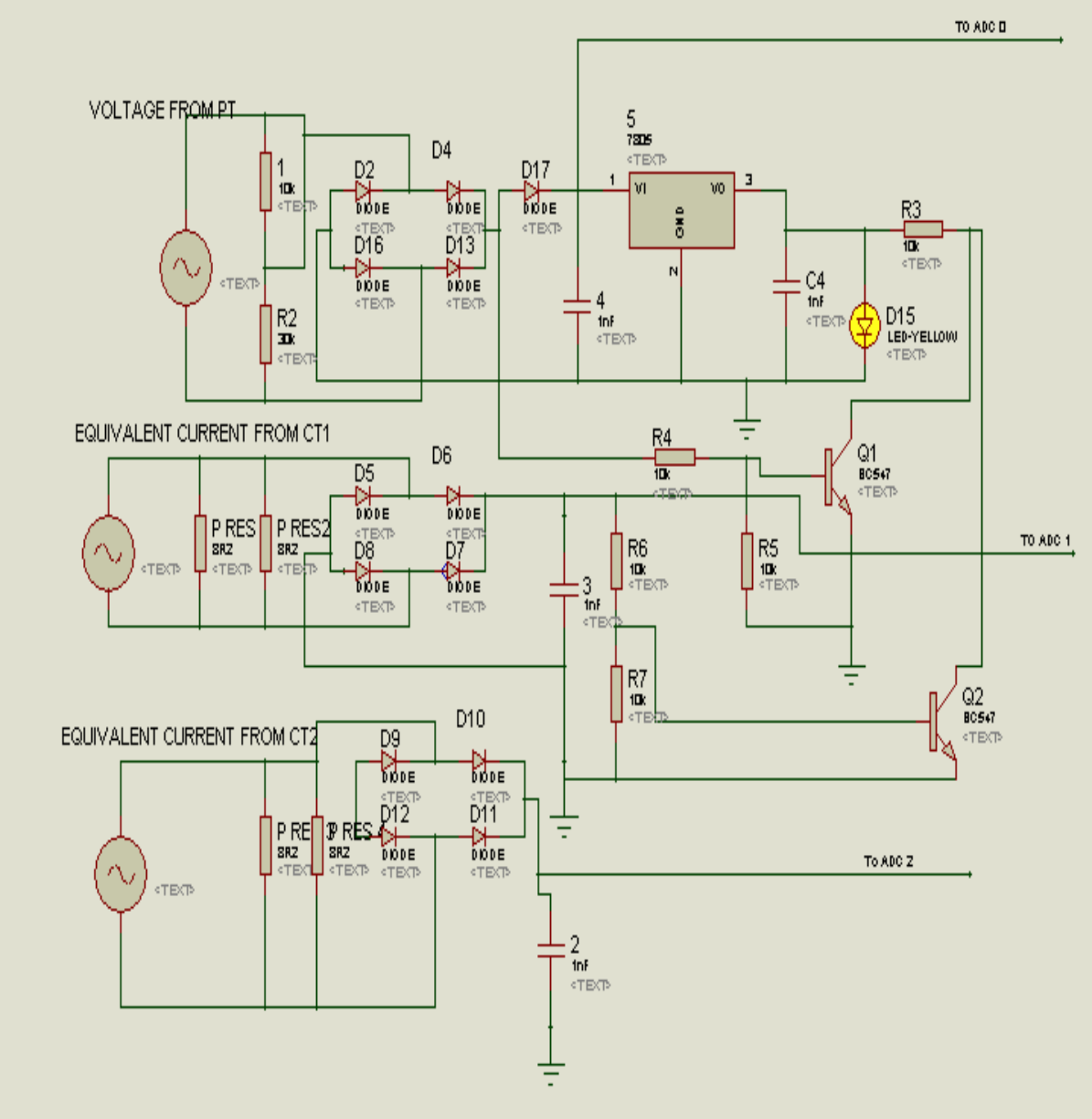

Figure 6: Zero crossing detection

The complete circuit diagram is shown in figure 7, with the intializations shown in the virtual terminal.

ISSN: 2277-9655
Impact Factor: 4.116

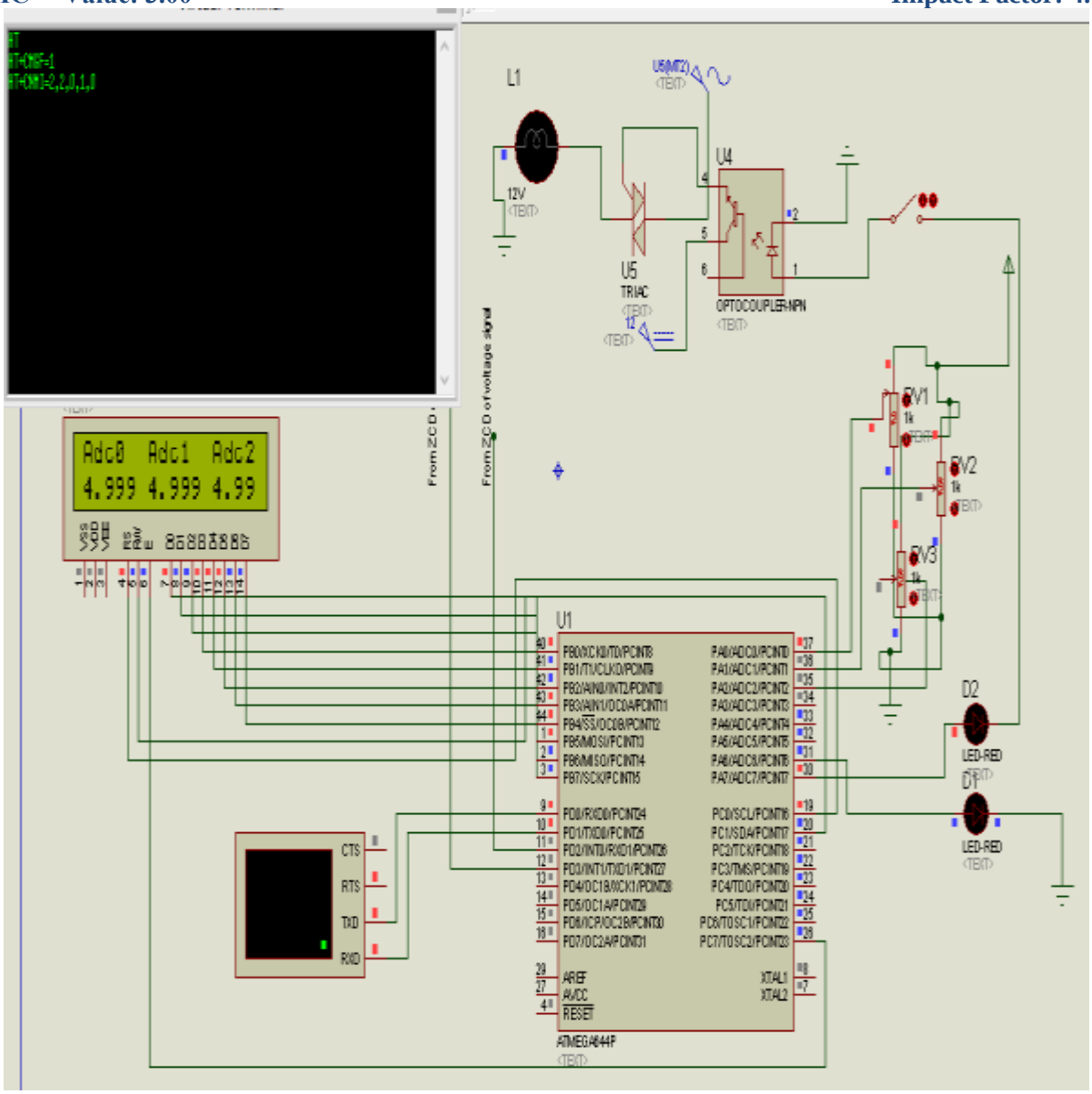

Figure 7: Circuit diagram of the proposed system.

The output at the server end is shown in the figure 8 which can be observed on the monitor or the display available.

Figure 8. Output at the server end.

ISSN: 2277-9655
Impact Factor: 4.116

CONCLUSION AND FUTURE WORK

GSM based device which we designed is easy to installation and beneficial for both energy supply authority and consumer. It also provide additional feature such as power disconnect due to outstanding dues, power cut alert, tempering alert. It also gives the information of total load used in a house on request at any time and sends a SMS alert to energy provider company. The statistical load used and profile can help customer manage their energy consumption. This system is secure and reliable because it can be accessed only by an authorized person. If any un-authorized person tries to access the system this system send an alert to energy provider. This device has the capability to revolutionize the energy meter market and will become help to country revenue by stopping the current theft and punishing the dishonest customers. Energy metering of our system that provide more solutions for implementing multiple layers of tamper detection implemented as a part of hardware and software solution. The theft such as double feeding are analyzed directly by the nearest substation with the help of PLCC where contact resistance test is used to detect by passing digital signal of required frequency.

Further Enhancement

1. Missing Potential

This is a common connection fraud usually deployed in three phase energy meters where the voltage component for one of the phases is made zero by removing one of the phase wires from the meter terminal. This results in recording less energy consumption as consumption from one of the phases becomes zero (P = V x I where V= 0).During this condition since the voltage is absent and current is present, the logic is easily able to sense this and record as tamper event if condition persists for certain duration.

2. **Automatic billing invoice**

By the introduction of real time clock (RTC) automatic meter reading can be designed.Which automatically evaluates the tariff of the corresponding customer and needs of task force will be eliminated. The overall combinational design leads smart metering.

REFERENCES

[1] J.Nagi, K.S.Yap, S.K.Tiong, S.K.Ahmed, Malik Mohamad, “Non Technical Loss Detection for Metered consumers using support vector machines”, IEEE transactions on Power Delivery, Vol.25, No.2, Pg. 1162-1171, April 2010
[2] A.S.Pabla, “Electric Power Distribution”, Pg. 213-215, Fifth Edition, Eleventh Reprint, Tata McGraw Hill Publications, 2008
[3] Guhesh Swaminathan ;Maheedar Subramanian ; Pravin Thangaraj"Distribution line monitoring system for the detection of power theft using power line communication ”, Energy Conversion (CENCON), 2014 IEEE Conference onpage 55 – 60 13-14 Oct. 2014 page 55 – 60
[4] International Journal of Electrical and Electronics Engineering (IJEEE) ISSN (PRINT): 2231 – 5284, Vol.1, Issue 3, 2012
[5] Annual report of Nepal Electricity Authority,2002-2014.